# Tight bounds for rational sums of squares over totally real fields

Ronan Quarez

# BOUNDING THE RATIONAL SUMS OF SQUARES OVER TOTALLY REAL FIELDS

RONAN QUAREZ

Abstract. Let $K$ be a totally real Galois number field. C. J. Hillar proved that if $f \in \mathbb{Q}[x_1, \dots, x_n]$ is a sum of $m$ squares in $K[x_1, \dots, x_n]$, then $f$ is a sum of $N(m)$ squares in $\mathbb{Q}[x_1, \dots, x_n]$, where $N(m) \le 2^{[K:\mathbb{Q}]+1} \cdot \binom{[K:\mathbb{Q}]+1}{2} \cdot 4m$, the proof being constructive.

We show in fact that $N(m) \le (4[K:\mathbb{Q}]-3) \cdot m$, the proof being constructive as well.

## 1. Introduction

In the theory of semidefinite linear programming, there is a question by Sturmfels

**Question 1.1** (Sturmfels)**.** If $f \in \mathbb{Q}[x_1, \dots, x_n]$ is a sum of squares in $\mathbb{R}[x_1, \dots, x_n]$, then is $f$ also a sum of squares in $\mathbb{Q}[x_1, \dots, x_n]$ ?

Hillar ([3]) answers the question in the case where the sum of squares has coefficients in a totally real Galois number field :

**Theorem 1.2** (Hillar)**.** *Let $f \in \mathbb{Q}[x_1, \dots, x_n]$ be a sum of $m$ squares in $K[x_1, \dots, x_n]$ where $K$ is a totally real Galois extension of $\mathbb{Q}$. Then, $f$ is a sum of*

$$2^{[K:\mathbb{Q}]+1} \cdot \binom{[K:\mathbb{Q}]+1}{2} \cdot 4m$$

*squares in $\mathbb{Q}[x_1, \dots, x_n]$.*

The aim of this note is to show, modifying a little bit Hillar's proof, that only $(4[K:\mathbb{Q}]-3) \cdot m$ squares are needed (that is Theorem 3.1). Moreover, as in [3], the argument is constructive.

## 2. Hillar's method

Having in mind the Lagrange's four squares Theorem, we focus ourselves on *rational sum of squares* i.e. linear combination of squares with positive rationnal coefficients.

Let $K$ be a totally real Galois extension of $\mathbb{Q}$ which we write $K = \mathbb{Q}(\theta)$ with $\theta$ a real algebraic number, all of whose conjugates are also real. We set $r = [K:\mathbb{Q}]$ and $G = \mathrm{Gal}(K/\mathbb{Q})$.

Let $f \in \mathbb{Q}[x_1, \dots, x_n]$ be a sum of $m$ squares in $K[x_1, \dots, x_n]$, namely $f = \sum_{k=1}^{m} f_k^2$, with $f_k \in K[x_1, \dots, x_n]$. Summing over all actions of $G$ (i.e. "averaging"), we get

*Date*: July 14, 2009.

2000 *Mathematics Subject Classification.* 12Y05, 12F10, 11E25, 13B24.

*Key words and phrases.* Rational sum of squares, semidefinite programming, totally real number field.

$$f = \frac{1}{\mid G \mid} \sum_{k=1}^{m} \sum_{\sigma \in G} (\sigma f_k)^2 \tag{1}$$

Next, we write each $f_k$ in the form

$$f_k = \sum_{i=0}^{r-1} q_i \theta^i$$

where $q_i \in \mathbb{Q}[x_1, \ldots, x_n]$. Then,

$$\sum_{\sigma \in G} (\sigma f_k)^2 = \sum_{j=1}^{r} \left( \sum_{i=0}^{r-1} q_i (\sigma_j \theta)^i \right)^2 \tag{2}$$

We may write this sum of squares as the following product of matrices

$$\begin{pmatrix} q_0 \\ \vdots \\ q_{r-1} \end{pmatrix}^T \begin{pmatrix} 1 & \sigma_1\theta & \ldots & (\sigma_1\theta)^{r-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_r\theta & \ldots & (\sigma_r\theta)^{r-1} \end{pmatrix}^T \begin{pmatrix} 1 & \sigma_1\theta & \ldots & (\sigma_1\theta)^{r-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_r\theta & \ldots & (\sigma_r\theta)^{r-1} \end{pmatrix} \begin{pmatrix} q_0 \\ \vdots \\ q_{r-1} \end{pmatrix}$$

We obtain what is called a Gram matrix (cf [1]) associated to the sum of squares in (2). Let

$$G = \begin{pmatrix} 1 & \sigma_1\theta & \ldots & (\sigma_1\theta)^{r-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_r\theta & \ldots & (\sigma_r\theta)^{r-1} \end{pmatrix}^T \begin{pmatrix} 1 & \sigma_1\theta & \ldots & (\sigma_1\theta)^{r-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_r\theta & \ldots & (\sigma_r\theta)^{r-1} \end{pmatrix}$$

Note that the entries of $G$ are in $\mathbb{Q}$ since they are invariant under the $\sigma_j$'s.

Now, we come to the slight modification of the proof of Hillar that will improve the bound.

## 3. LU-decomposition of the Gram matrix

If $u(x)$ denotes the minimal polynomial of the Galois extension $K$ over $\mathbb{Q}$, then the $(i, j)$-th entry of the matrix $G$ is the $i + j - 2$-th Newton sum of $(\sigma_1, \ldots, \sigma_r)$ the roots of $u(x)$. It is well known that the rank of $G$ is equal to $r$ and its signature (the difference between the positive eigenvalues and the negative ones) is equal to the number of real roots of $u(x)$ (see for instance [2, Theorem 4.57]). In our case, we readily deduce that $G$ is a positive definite matrix since $K$ is totally real. Thus, all its principal minors are different from zero (they are strictly positive !) and $G$ admits a LU-decomposition which we may put in a symmetric form

$$G = U^T D U$$

where $D$ is diagonal and $U$ is upper triangular with diagonal identity, and $U, D$ have rational entries.

We may view this decomposition as a matricial realization of the Gauss algorithm which reduce the quadratic form given by $G$.

Now, if we denote by $f_1, \ldots, f_r$ the polynomials in $\mathbb{Q}[x_1, \ldots, x_r]$ appearing as the rows of the matrix $U \times \begin{pmatrix} q_0 \\ \vdots \\ q_{r-1} \end{pmatrix}$ and by $d_1, \ldots, d_r$ the rational entries onto the diagonal of $D$, then we get from (2) the identity :

$$\frac{1}{\mid G \mid} \sum_{\sigma \in G} (\sigma f_k)^2 = \frac{d_1}{\mid G \mid} g_1^2 + \ldots + \frac{d_r}{\mid G \mid} g_r^2 \tag{3}$$

This construction leads to

**Theorem 3.1.** *Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$ be a sum of $m$ squares in $K[x_1, \ldots, x_n]$, where $K$ is a totally real Galois extension of $\mathbb{Q}$. Then, $f$ is a sum of $(4[K : \mathbb{Q}] - 3) \cdot m$ squares in $\mathbb{Q}[x_1, \ldots, x_n]$.*

*Proof.* By (1) and (3), it suffices to apply Lagrange's four squares Theorem to get that $f$ is a sum of $4[K : \mathbb{Q}] \cdot m$ squares in $\mathbb{Q}[x_1, \ldots, x_n]$.

But let us note that the first diagonal entry of $D$ is always $d_1 = r = [K : \mathbb{Q}]$. Then, by the averaging process the first coefficient appearing in the rational sum of squares in (3) is $\frac{d_1}{|G|} = 1$ : already a square in $\mathbb{Q}$ ! Whereas the others coefficients $\frac{d_i}{|G|}$ in the rational sum of squares could be any positive rational which we rewrite as a sum of 4 squares. This concludes the proof. $\square$

*Remark* 3.2. Beware that if we perform the Cholesky algorithm to the matrix $G$ instead of the LU-decomposition, it yields a factorisation $G = U^T U$ where $U$ is lower triangular but with entries in $\mathbb{Q}[\sqrt{d_1}, \ldots, \sqrt{d_r}]$ for some integers $d_1, \ldots, d_r$. Then, an averaging argument would produce identities over $\mathbb{Q}$ but will raise the number of squares by an unexpected multiplicative factor $2^{[K:\mathbb{Q}]}$.

Let us consider as an example, the simple case of quadratic extensions :

**Example 3.3.** Let $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Q}$ is not a square. The extension $K$ is always Galois, and it is totally real if $d \geq 0$.

Let $f \in \mathbb{Q}(x_1, \ldots, x_n)$ be such that $f = \sum_{k=1}^{m} (a_k + b_k\sqrt{d})^2$ with $a_k, b_k \in \mathbb{Q}(x_1, \ldots, x_n)$. Since $f$ has rational coefficients, by averaging we get

$$f = \frac{1}{2} \sum_{k=1}^{m} (a_k + b_k\sqrt{d})^2 + (a_k - b_k\sqrt{d})^2 = \sum_{k=1}^{m} (a_k^2 + d b_k^2)$$

It remains to write $d$ as a sum of $l \leq 4$ squares of rationals, and we get that $f$ is a sum of at most $(1 + l) \cdot m$ squares in $\mathbb{Q}(x_1, \ldots, x_n)$.

As another illustration, we apply our method to [3, Example 1.7] :

**Example 3.4.** Consider the polynomial

$$f = 3 - 12y - 6x^3 + 18y^2 + 3x^6 + 12x^3y - 6xy^3 + 6x^2y^4$$

which is the following sum of squares

$$f = (x^3 + \alpha^2 y + \beta x y^2 - 1)^2 + (x^3 + \beta^2 y + \gamma x y^2 - 1)^2 + (x^3 + \gamma^2 y + \alpha x y^2 - 1)^2$$

in $\mathbb{Q}(\alpha)[x, y]$ where $\alpha, \beta, \gamma$ are the real roots of the polynomial $u(x) = x^3 - 3x + 1$.

We do not need to average and directly compute the matrix $G$ and its symmetric LU-decompositon

$$\begin{pmatrix} 3 & 0 & 6 \\ 0 & 6 & -3 \\ 6 & -3 & 18 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & -\frac{1}{2} & 1 \end{pmatrix} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & \frac{9}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix}$$

Because of the relations $\beta = 2 - \alpha - \alpha^2$ and $\gamma = \alpha^2 - 2$, the vector of polynomials $q = (q_0, q_1, q_2)^T$ is $q = (x^3 + 2xy^2 - 1, -xy^2, y - xy^2)^T$ and hence

$$f = 3\left((x^3 + 2xy^2 - 1) + 2\,(y - xy^2)\right)^2 + 6\left(-xy^2 - \frac{1}{2}(y - xy^2)\right)^2 + \frac{9}{2}\left(\, y - xy^2\right)^2$$

a rationnal sum of 3 squares, to compare with the rational sum of 6 squares obtained in [3].

## References


[1] M.D. Choi, T.Y. Lam, B. Reznick, *Sums of squares of real Polynomials*, Proc. Sympos. Pure Math., 58, Part 2, Amer. Math. Soc., Providence, RI, 1995.

[2] S. Basu, R. Pollack, M.F. Roy, *Algorithms in Real Algberaic Geometry*, Springer

[3] C. J. Hillar, *Sums of squares over totally real fields are rational sums of squares*, Proc. Amer. Math. Soc. 137 (2009), no. 3, 921–930.



IRMAR (CNRS, URA 305), Université de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex, France

*E-mail address*: `e-mail : ronan.quarez@univ-rennes1.fr`